

信息系统 (IS) 审计和鉴证的专业性以及完成此类工作所需的技术需要专门适用于 IS 审计和鉴证的标准。IS 审计和鉴证标准的发展和传播是 ISACA[®] 对审计业界作出专业贡献的基础。

IS 审计和鉴证标准定义 IS 审计和报告的强制性要求，并告知：

- 根据 ISACA 职业道德规范中关于职业责任的规定，IS 审计和鉴证专业人员的执行绩效所应达到的最低标准
- 管理层和其他利益方对执业者在专业工作上的期望
- 注册信息系统审计师 (CISA[®]) 认证持有人的特定要求。如果 CISA 认证持有人未能遵守这些标准，则可能会导致 ISACA 董事会或适当的委员会对其行为进行调查，进而采取相应的纪律措施。

IS 审计和鉴证专业人员应当根据情况在其工作底稿中包括一项声明，说明已根据 ISACA IS 审计和鉴证标准或其他适用的专业标准完成该项业务。

适用于 IS 审计和鉴证专业人员的 ITAF[™] 框架提供了多层次的指引：

- **标准**，分为三类：
 - 通用标准（1000 系列）——是 IS 审计和鉴证专业人员的工作指导原则。这些标准适用于所有任务的执行，而且还涉及到 IS 审计和鉴证专业人员的道德、独立性、客观性和应有的审慎性，以及知识、职业能力和技能。标准声明（其中**粗体**部分）是强制性的。
 - 履行标准（1200 系列）——涉及到任务执行，例如，规划与监督、任务范围、风险与重要性、资源调动、监督与任务管理、审计与鉴证证据，以及专业判断和应有的审慎性。
 - 报告标准（1400 系列）——涉及到报告类型、沟通方式以及传达的信息
- **准则**，支持标准，并且同样分为三类：
 - 通用准则（2000 系列）
 - 履行准则（2200 系列）
 - 报告准则（2400 系列）
- **工具和技术**，为 IS 审计和鉴证专业人员提供附加指导，如白皮书、IS 审计/鉴证计划和 COBIT[®] 5 产品系列

ITAF 中所使用的在线术语表请参见 www.isaca.org/glossary。

免责声明：ISACA 设计的此指南是根据 ISACA 职业道德规范中关于职业责任的规定所应达到的最低绩效水平。ISACA 不断言使用此产品将保证带来成功的结果。该出版物不应当被视为包含所有合适的程序或测试，或排除通过合理引导获得相同结果的其他程序或测试。在确定任何具体程序或测试是否适当时，控制或专业人员应当对特定系统或 IS 环境呈现的具体控制情况作出其独立的专业判断。

ISACA 专业标准和职业管理委员会 (PSCMC) 为准备标准和指南，致力于进行广泛的磋商。在发布任何文件之前，会在全球领域公布一份征求意见稿，以征求公众的意见。反馈意见也可以通过电子邮件 (standards@isaca.org)、传真 (+1.847. 253.1443) 或邮件 (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA) 等方式向专业标准开发总监提交。

ISACA 2012-2013 专业标准和职业管理委员会

Steven E. Sizemore, CISA, CIA, CGAP, 主席	Texas Health and Human Services Commission, 美国
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, 英国
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, 美国
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, 马来西亚
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, 新西兰
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., 日本
Ian Sanderson, CISA, CRISC, FCA	NATO, 比利时
Timothy Smith, CISA, CISSP, CPA	LPL Financial, 美国
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., 阿根廷

IS 审计和鉴证标准 1401 报告

声明

- 1401.1** 在完成项目后，IS 审计和鉴证专业人员应以报告通报结果，其内容包括：
- 企业名称、报告的目标接收者以及内容和流通方面的任何限制
 - 项目的范围、目标和涵盖的时间段以及所执行工作的性质、时间选择和程度范围
 - 发现、结论和建议
 - IS 审计和鉴证专业人员在执行该项目方面所具有的任何资质或范围限制
 - 签名、日期以及按审计章程或约定书之条款进行的分发
- 1401.2** IS 审计和鉴证专业人员应当确保审计报告中所列的发现具有充分且适当的证据予以支持。
-

重要方面

- IS 审计和鉴证专业人员应当：
- 获得被审计单位提供的书面声明，其中明确详述项目的关键领域、出现的问题及其解决方案以及被审计单位作出的认定
 - 确定被审计单位的声明已经过被审计单位签字并署明日期，以表示承认其在项目方面的职责
 - 在工作底稿中记录并保留在执行项目过程中所收到的任何书面或口头的声明。对于鉴证项目，从被审计单位获取的声明应当采用书面形式，以减少可能产生的误解。
 - 定制报告的形式和内容，以支持所执行的项目的类型，如：
 - 审计（直接或证明）
 - 审核（直接或证明）
 - 商定的程序
 - 在报告中描述重大或重要缺陷及其对实现项目目标的影响。
 - 在定稿和发布之前与有关的管理层讨论报告草案的内容，并根据情况在最终报告中包含管理层对发现、结论和建议的反馈。
 - 向治理负责人，并根据情况向主管部门通报控制环境中的重要缺陷和重大漏洞，并在报告中披露已通报的内容。
 - 在最终报告中引用任何相关的报告。
 - 向被审计单位管理层通报不够严重但并非无关紧要的内部控制缺陷。此时，应当通知治理负责人或主管部门，已向被审计单位管理层通报此类控制缺陷。
 - 识别执行项目过程中应用的标准，并根据情况通报不符合这些标准的任何情况。
-

术语

术语	定义
相关信息	与控制有关，向评估员告知有关基础控制或控制组件运行情况的有用信息。直接确认控制运行情况的信息最为相关。间接涉及控制运行情况的信息也可能相关，但不如直接信息。参见 COBIT 5 信息质量目标
可靠信息	准确、可考证和来自客观来源的信息。参见 COBIT 5 信息质量目标
足够信息	当评估员已收集足够的信息，可以得出合理的结论时，即为足够。然而，信息若要足够，它首先必须是合适的。参见

IS 审计和鉴证标准 1401 报告

	COBIT 5 信息质量目标
合适信息	相关（即适合预期目的）、可靠（即准确、可检验和来自客观来源）和及时（即在适当的时限内产生和使用）的信息。参见 COBIT 5 信息质量目标
及时信息	有可能在对企业产生重大影响之前预防或检测控制缺陷的时限内产生和使用。参见 COBIT 5 信息质量目标

关联标准和准则

类型	标题
准则	2401 报告

生效日期

本 ISACA 标准自 2013 年 11 月 1 日起对所有 IS 审计和鉴证业务生效。